Department of Defense

INSTRUCTION

NUMBER 5210.74

June 26, 1985

Administrative Reissuance Incorporating Change 1, November 16, 1994

ASD(C3I)

SUBJECT: Security of Defense Contractor Telecommunications

References: (a) National Communications Security Instruction (NACSI) 6002, "Protection of Contractor Telecommunications," June 4, 1984
(b) National Security Decision Directive (NSDD) 145, "National Policy on Telecommunications and Automated Information Systems Security," September 17, 1984
(c) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," October 6, 1981
(d) through (i) see enclosure E1.

1. PURPOSE

This Instruction:

1.1. Implements reference (a) by providing implementation guidance on a new means to expedite securing and protecting certain telecommunications between and among DoD Components, their contractors, and subcontractors.

1.2. Provides a new method for direct acquisition of COMSEC and approved protection equipment, for contractor installation and maintenance of service, and for recovery of costs through the contract.

1.3. Provides further definition of the telecommunications involved and the priority to be assigned to the program of securing and protecting those telecommunications.

1.4. Establishes policy and procedures and assigns responsibilities for security of

DoD contractor telecommunications.

2. APPLICABILITY AND SCOPE

This Instruction:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies, (hereinafter referred to as DoD Components).

2.2. Applies to existing and future contracts executed by DoD Components that involve classified information or unclassified national security-related (sensitive) information, as defined herein.

2.3. Applies to United States Defense contractor telecommunications, worldwide where the use of COMSEC or protection equipment of U.S. manufacture is permitted.

3. DEFINITIONS

Terms used in this Instruction are contained in enclosure E2.

4. POLICY

It is DoD policy to secure or protect telecommunications among and between the DoD Components, their contractors, and subcontractors in a manner that will preclude potential damage to the national defense. NSDD 145 (reference (b)), DoD Directive C-5200.5 (reference (c)), and DoD Directive 5220.22 (reference (d)) apply.

5. PRIORITIES.

The following priorities apply:

5.1. First priority shall be given to providing a secure voice capability among the DoD program managers, and their contractors and subcontractors who currently are performing on classified contracts and possess or routinely exchange significant amounts of classified information.

5.2. Second priority, if not concurrent with the first priority, shall be given to

securing record and data telecommunications among the DoD program managers and their contractors and subcontractors who currently are performing on classified contracts and possess or routinely exchange significant amounts of classified information.

5.3. Third priority shall be given to protecting unclassified national security-related voice, record, and data telecommunications among program managers and their contractors and subcontractors.

6. RESPONSIBILITIES

6.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall oversee the implementation of this Instruction.

6.2. The Deputy Under Secretary of Defense for Policy shall issue appropriate changes to DoD 5220.22-R (reference (e)), and review implementing directives, instructions, and procedures of the DoD Components for compliance.

6.3. The Deputy Under Secretary of Defense for Acquisition Management shall ensure that the requirements of this Instruction are incorporated into the Federal Acquisition Regulations (reference (i)).

6.4. The Director, Defense Investigative Service, shall ensure the provisions of this Instruction that pertain to securing of classified telecommunications are incorporated in DoD 5220.22-R (reference (e)).

6.5. The Secretaries of the Military Departments, the Chairman, Joint Chiefs of Staff and the Directors of Defense Agencies shall:

6.5.1. Formulate and issue directives, instructions, and procedures to implement the provisions of this Instruction within their respective DoD Components.

6.5.2. Provide an assessment of progress in accordance with NSDD 145 (reference (b)) and Section IV of NTISS Directive 900, (reference (h)).

6.5.3. Develop key management plans for both secure and protected applications and provide keying material requirements to the Director, NSA, in accordance with normal procedures.

6.6. The Director, National Security Agency shall:

6.6.1. Establish a program to provide for the direct acquisition of COMSEC and approved protection equipment.

6.6.2. Publish a list of sources and pricing guidelines for this program quarterly.

6.6.3. Ensure there are no conflicts with DoD COMSEC production contracts.

6.6.4. Provide technical assistance, guidance, and doctrine for both secure and protection systems and services.

6.6.5. Provide keying material in support of DoD Component key management plans.

7. PROCEDURES

The following general guidelines apply in implementing this policy:

7.1. These procedures supplement but do not replace traditional methods for acquisition and installation of COMSEC equipment on Defense contractor telecommunications. DoD Components are encouraged to use this new approach, traditional Government Furnished Equipment (GFE) methods, or any combination deemed most likely to achieve the earliest possible attainment of policy objectives.

7.2. Each DoD contract shall contain a specific statement of any additional requirements for securing or protecting telecommunications as specified in subpart 4.5 of the Federal Acquisition Regulation, (reference (i)), and shall include authorization for direct purchase of equipment or services from vendors or manufacturers, by expressing the following type of information:

7.2.1. This contract requires the securing of classified information by employing secure voice telecommunications between (enter specific details). The contractor is authorized to procure COMSEC equipment and services directly from COMSEC vendors identified by NSA.

7.2.2. This contract requires the securing of classified information by employing secure data or record telecommunications between (enter specific details). The contractor is authorized to procure COMSEC equipment and services directly from COMSEC vendors identified by NSA.

7.2.3. This contract requires both the securing of classified information and the protection of unclassified national security-related information. For the former, the contractor shall employ secure (voice, data, and record, as appropriate) telecommunications between (enter specific details), and is authorized to procure COMSEC equipment and services directly from COMSEC vendors identified by NSA. For the latter, the contractor shall employ protected (voice, data, and record, as appropriate) telecommunications between (enter specific details), and is authorized to procure NSA-approved protection equipment and services directly from vendors identified by NSA.

7.2.4. This contract requires the protecting of unclassified national security-related information by employing protected voice, data, or record telecommunications between (enter specific details). The contractor is authorized to procure NSA-approved protection equipment and services directly from vendors identified by NSA.

7.3. When contracts call for COMSEC equipment, the contractor shall use the contract clause (paragraphs 7.2.1., 7.2.2., or 7.2.3. as applicable) as authorization to procure COMSEC equipment and related services directly from the vendor. DoD Components may purchase secure systems directly from NSA-approved vendors for the Government terminals of Defense contractor telecommunications.

7.4. When contracts call for protection equipment and services, the contractor may purchase NSA-approved protection equipment and services directly from the vendors. Protection equipment and keying material are unclassified and not under the purview of the DoD Industrial Security Program. However, NSA-produced or -approved keying material must be used.

7.5. New and existing DoD contracts shall incorporate the procedures of this Instruction. Existing contracts shall be modified as necessary, but no later than 12 months from the effective date of this Instruction or the Federal Acquisition Regulation, (reference (i)).

7.6. Costs for acquisition, operation, maintenance, and administration for both secure and protected systems and services will be recovered in accordance with the Federal Acquisition Regulation (reference (i)) in the same manner as costs for physical security requirements. Keying material for both secure and protected systems will be furnished by NSA at no charge. DoD Components are responsible for developing keying material requirements for themselves and their associated contractors for both

secure and protected applications and providing information to the Director, NSA, in accordance with normal procedures.

7.7. All COMSEC equipment, that is acquired directly from an approved vendor by a DoD contractor is U.S. Government property and subject to disposition instructions upon termination of the contract. It is the intent of this Instruction that COMSEC equipment obtained under these procedures be retained by the contractor for use on future contracts with DoD or any other Federal activity listed in Section 1 of the DoD Industrial Security Regulation. DoD Components are responsible for coordinating retention or disposition in accordance with DoD 5220.22-R (reference (e)).

7.8. Protection equipment obtained under these procedures shall become the property of the contractor.

8. EFFECTIVE *DATE*

This Instruction is effective *immediately*.

Donald C. Latham
Assistant Secretary of Defense
(Command, Control, Communications
and Intelligence)

Enclosures - 2

1. References, continued
2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

(d) DoD Directive 5220.22, "DoD Industrial Security Program," December 8, 1980
(e) DoD 5220.22-R, "Industrial Security Regulation," February 1984 authorized by reference (d), above
(f) DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information, March 1984, authorized by reference (d), above
(g) DoD 5220.22-S-1, "COMSEC Supplement to Industrial Security Manual for Safeguarding Classified Information," August 1983, authorized by reference (d), above
(h) National Telecommunications and Information Systems Security (NTISS) Directive 900, "Governing Procedures of the National Telecommunications and Information Systems Security Committee," February 1, 1985
(i) Federal Acquisition Regulation, Subpart 4.5, "Security of Defense Contractor Telecommunications" (to be issued)

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. COMSEC Vendor. A manufacturer of COMSEC equipment or services who is specifically authorized in writing, by the Director, NSA, to sell such equipment and related services to DoD Components, or their contractors and subcontractors.

E2.1.2. Defense contractor telecommunications. Voice, record, and data communications, employed between and among the DoD Component program managers and their contractors and subcontractors. This includes management information systems and local data networks that connect to external transmission media.

E2.1.3. NSA-Approved Protection. Equipment or techniques that the Director, NSA, has determined to meet certain prescribed Federal security standards for unclassified national security-related telecommunications protection.

E2.1.4. Protecting. The application of National Security Agency (NSA)-approved protection equipment, devices, or techniques to Defense contractor telecommunications over which unclassified national security-related information is transmitted.

E2.1.5. Securing. The application of National Security Agency (NSA)-approved COMSEC equipment, devices, or techniques to telecommunications systems that transmit classified information.

E2.1.6. Unclassified National Security-Related Information. Information incident to the performance of contracts with Department of Defense that involve technologies listed in the current edition of "The Militarily Critical Technologies List" published in unclassified form by the Office of the Under Secretary of Defense for Research and Engineering, and other Government or Government derived unclassified information deemed by DoD Components or their contractors to require protection.